

C L A I M S

1 1. A security system for controlling access to one or more
2 application functions located on a server or accessible
3 via server, each application function having an
4 associated security level, wherein one or more clients
5 communicate with said server by means of requests for
6 accessing one of said application functions using a
7 network, wherein access to said application functions is
8 controlled by security requirements, comprising:

9 an authentication component functionally separated from
10 said clients and said application functions for
11 processing said client request independently of said
12 client type, containing more than one authentication
13 mechanisms and selecting and executing an authentication
14 mechanism from said more than one authentication
15 mechanisms based on the information contained in the
16 client request resulting in a security state;

17 a security component containing a security policy
18 describing security requirements (security level) for
19 accessing application functions, comparing said security
20 state associated with said client with the security level
21 of the application function and allowing access to the
22 application function if the security state fulfills the
23 security level.
24

1 2. A system according to claim 1, wherein said clients are
2 PVC-devices.

3 3. A system according to claim 1, wherein said
4 authentication component and said security component are
5 integrated in one component stored on a server.

1 4. A system according to claim 1, whereby said
2 authentication component consists of security plug-ins
3 whereby each authentication mechanism is laid down in a
4 separate security plug-in.

1 5. A system according to claim 4, whereby the authentication
2 mechanism may be UserID/Password, Challenge/Response or
3 digital signature.

6 6. A system according to 2 further comprising:
7
8 a component (ADL) for converting PVC-device specific
9 requests into canonical requests before said request is
10 used by said authentication component.

11 7. A method for controlling access to one or more
1 application functions stored on a server or accessible
2 via server, each application function having an
3 associated security level, wherein one or more clients
4 communicate with said server by means of requests for
5 accessing one of said application functions using a
6 network, whereby access to said application functions is
7 controlled by a security requirements, comprising the
8 steps of:
9

10 routing all incoming requests created by said clients to
11 an authentication component which is functionally

12 independent from said clients and said application
13 functions, said authentication component comprising the
14 steps of:

15 authentication of said client by determining an
16 authentication mechanism provided by said authentication
17 component by means of authentication information
18 contained in said request and applying said
19 authentication mechanism;

20 storing a result of said authentication and said
21 authentication information or parts of it contained in
22 said request as a security state;

23
24 using security requirements for said one of said
25 application functions to be accessed;

26 comparing said stored security state with said security
27 requirements for accessing the requested application
28 function ; and .

29 invoking said requested application function if said
30 security state fulfills said security requirements.

1 8. A method according to claim 7 wherein said incoming
2 requests are canonical requests.

1 9. A method according to claim 8 wherein said canonical
2 requests are created by a Device Adaptation Layer which
3 converts client specific requests into canonical
4 requests.

1 10. A method according to claim 7 comprising the further
2 steps of:

3 creating a session identifier when establishing a
4 communication between a client and a server and using
5 said session identifier in all requests and responses
6 between said client and said server.

1 11. A method according to claim 10 whereby said session
2 identifier and said security state are placed in a
3 cookie, whereby said cookie is inserted into each
4 request and response between said client and said server.

1 12. A method according to claim 7 wherein said clients are
2 PVC-devices.

1 13. A computer program comprising computer program code
2 portions for performing respective steps of the method
3 according to claim 7 to 12 when the program is executed
4 in a computer.

1 14. A computer program product stored on a computer-readable
2 media containing software code for performing of the
3 method according to one of the claim 7 to 12 if the
4 program product is executed on the computer.

1 15. A client-server system, wherein one or more clients,
2 having client types, communicate with a server by means
3 of requests for accessing application functions located
4 on or accessible via said server, wherein access to said

application functions is controlled by a security system located on said server, wherein said security system comprises:

an authentication component, functionally separated from said one or more clients and said application functions for processing client requests independently of client type, containing one or more authentication mechanisms and selecting and executing an authentication mechanism from said authentication mechanisms based on the information contained in the client request, resulting in a security state;

a security component containing a security policy describing security requirements (security level) for accessing application functions, comparing said security state associated to a client with the security level of the application function and allowing access to the specified application function if the security state fulfills the security level.